Defense-in-Depth Strategy

Michael Allred - State of Utah

2005 Annual Security Conference
Digital Citizenship - Utah at Risk

March 7 - 8, 2005

Utah!
Where ideas connect™

Sponsored by

UEN
UTAH EDUCATION NETWORK
WWW.UEN.ORG

UTAH STATE OFFICE OF EDUCATION

ITS Customer Driven Technology
Information Technology Services

Defense-In-Depth Strategy for the State of Utah

Michael Allred
Chief Information Security Officer
December 2004

ITS Customer Driven Technology
Information Technology Services

Defense-In-Depth Strategy
Why the need?

- ✓What are you most worried about?
- ✓What are you biggest security concerns?
- ✓What keeps you up at night?

ITS Customer Driven Technology
Information Technology Services

Defense-In-Depth Strategy
Why the need?

- ✓What are the threats today?
- ✓SpyWare
- ✓Identity Theft
- ✓Phising / Pharming
- ✓PDA/cell phone theft
- ✓Hacker
- ✓Disgruntled Employees

ITS Customer Driven Technology
Information Technology Services


BUSINESS REVIEW

Subscribe to the Print Edition | Get Headlines by E-mail

Home
Business Today
Markets
Media
Australia
Technology
Inside China
Asia & Pacific
World
Arts
Letters
Sport
Wine
Editor's insight
Politics
Opinion
Mail Messenger
Tools
Search
Advertising
Contact Us

Home > Technology > ChoicePoint: Data lost to Nigerian fraud, not a hack

ChoicePoint: Data lost to Nigerian fraud, not a hack

Francis Till

Last week saw a too rare -- and yet too familiar -- event in the data security industry: an admission by a large vendor, ChoicePoint, that customer data had been compromised.

First, some background.

ChoicePoint warehouses data -- including social security numbers, birth certicates, death certificates, insurance reports, marriage and divorce reports and other deeply personal information (it even offers DNA identification analysis through a subsidiary, Bode Technology Group) -- that allows clients to perform background and other security checks on customers, clients and prospective employees.

With 5,500 employees in nearly 60 locations and about 19 billion "public" records on file, the company is Big Brother, in at least the corporate realm, and it says of its mission that it provides "decision-making information that helps reduce fraud and mitigate risk."

Had John Davy been vetted through ChoicePoint, for example, New Zealand might have been spared one of its tawdrier interludes.

Among the vertical industry groups it services -- which include government and law enforcement -- is "telecommunications and technology" where it offers a number of solutions designed to protect against the "increasing occurrence of identity theft crimes and the extreme losses associated with such thefts." It's an expert in this sort of fraud and its prevention, long and short.

So when it disclosed on 15 February that its databanks had been compromised, allowing thieves to buy the identities of people on whom it kept records, the internet security community sat up in shock.

Few companies have been open about loss of data security and ChoicePoint, as a company with special concerns going to data security, was not an exception to this pattern.

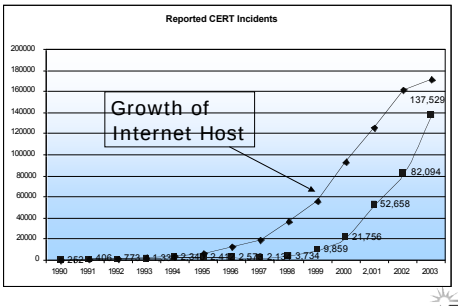
But it was required to notify California citizens under the state's breach notification act and only after doing so did it agree to notify potential victims in the rest of the country -- 145,000 of them in all.

Search Go

Technology

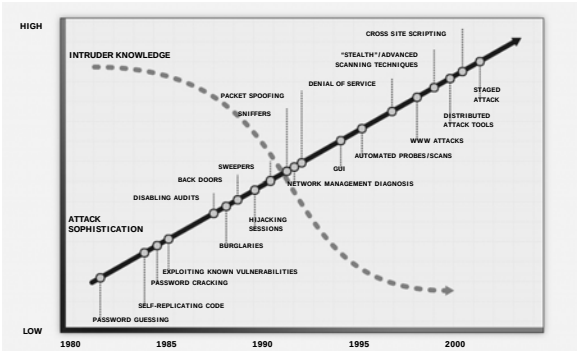
- Firefox growth slows
- Microsoft to companies: Here comes SP2, ready or not
- ChoicePoint: Data lost to Nigerian fraud, not a hack
- Comcorn fines restaurant operator $3k over neglected website
- Tech makeover: Technology drives business value
- Homeland Security coup for RoamAD: Data at any speed
- Symantec: No sitting duck target for Microsoft
- Is that you stuck to the web?
- Police net 41 possible kiddie porn offenders in national swoop
- Set your iPod free
- Personal email use at work hits productivity
- IBM paints a grim security picture for 2006

Growth of Incidents



ITS Customer Driven Technology

As systems get complex, attackers are less sophisticated…



Defense-In-Depth Strategy
Review

- ✓What should we do?
  - – Secure the network and the world we will a better place?
- ✓How many of you feel more secure because you have to take you shoes off at the airport?

Defense-In-Depth Strategy
Review

- A Defense-In-Depth Strategy Provides
  - ✓A holistic end-to-end security frameworks
  - ✓Layered approach
  - ✓Multiple points of security enforcement
  - ✓Keep it simple

Defense-In-Depth Strategy
Benefits

- A Defense-In-Depth Strategy Benefits
  - ✓Reduces an attackers chance of success
  - ✓Increase the probability of detection
  - ✓Contains the size of exposure
  - ✓Protects the confidentiality, integrity and availability (CIA) of critical state information and assets

Defense-In-Depth Strategy
Simplicity in our approach

- A Simplicity approach
  - ✓Routine technologies rather and depend on complex schemes
  - ✓Easier to protect, secure and maintain
  - ✓Easy to understand and implement

Defense-In-Depth Strategy

Example

- ✓ SpyWare
  - – Block Access to SpyWare sites
    - • Gator, Marketscore, Weatherbug
  - – Stop SpyWare Installations
    - • Drive by web installs
  - – Log and Report Activity
    - • Weekly SpyWare Reports
  - – Scan and remove from Desktop
  - – Inform and educate users
    - • "I just want a Finding Nemo screen saver"

Defense-In-Depth Strategy

Layered Approach

- ✓Policy, Procedures, and Awareness
- ✓Physical
- ✓Perimeter
- ✓Network
- ✓Systems
- ✓Applications
- ✓Data

Defense-In-Depth Strategy

Policy, Procedures and Awareness

- ✓Security Policies in place
- ✓Employees are trained and understand policies
- ✓Regular Review of Security Policies
- ✓Employee known their roles and responsibilities

Defense-In-Depth Strategy

The Human Factor

- More security processes than technology
- People will work around security if it is to complicated
- People are the weakest link, and the biggest threat is often from within.
- Employees often can make mistakes and be careless.
- Disgruntled, dissatisfied or careless employees can be a threat.
- Employee awareness, training and education are essential.

Defense-In-Depth Strategy

Physical Access and Environmental Controls

- ✓ Appropriately badge to enter protected areas.
- ✓ Physical locks to prevent access to systems.
- ✓ Physical layers or zones depending on security requirements.
- ✓ Multi factor authentication to access areas.
- ✓ Computers, desktops and data mediums are secured when not in use.
- ✓ Environmental controls ensure there is no damage to the critical systems.

Defense-In-Depth Strategy

Perimeter Defense

- ✓ Perimeter firewall protection.
- ✓ Logging, analysis, and reporting of attempted access
- ✓ Elimination of clear text and other services that can expose internal systems to external threats
- ✓ Encryption of incoming network traffic destined for more secure internal systems

Defense-In-Depth Strategy

Perimeter

- ✓ Bastion host and proxy services
- ✓ Authentication required for access to internal services
- ✓ Allow external traffic to specified networks
- ✓ External vulnerability assessments

Defense-In-Depth Strategy

Network

- ✓ Intrusion Detection
- ✓ Intrusion Prevention
- ✓ Network Segmentation
- ✓ Non-routable IP addresses
- ✓ Web content filtering
- ✓ Network based anti-virus
- ✓ Network vulnerability assessments
- ✓ Authentication required for network devices

Defense-In-Depth Strategy
Systems

- ✓ Standard system configurations
- ✓ Asset management
- ✓ Strong authentication
- ✓ Change control and management
- ✓ Patch and update management
- ✓ Host based intrusion detection
- ✓ Host based anti-virus
- ✓ Host based firewalls

Defense-In-Depth Strategy
Application

- ✓ Application development life cycle methodology
- ✓ Change control including peer and security reviews
- ✓ Authentication required applications layer
- ✓ Logging and audit build into application
- ✓ Email SPAM and virus filtering
- ✓ Risk review for new systems

Defense-In-Depth Strategy
Data

- ✓ Encrypted of data when stored
- ✓ Segmentation of data
- ✓ Authentication required to access data outside of application
- ✓ Authorization based on roles
- ✓ Logging, auditing and reporting of data access
- ✓ Limit access using access control list

Defense-In-Depth Strategy
Overview

A Defense-In-Depth Strategy Provides

- ✓ A holistic end-to-end security frameworks
- ✓ Layered approach
- ✓ Multiple points of security enforcement

DEFENSE-IN-DEPTH STRATEGY FOR THE STATE OF UTAH

October 2004, Version 1.0

This document defines the overall strategy for the State of Utah Security Model. A Defense-in-Depth strategy provides a holistic end-to-end security framework for the State infrastructure, layering several security components to achieve multiple points of security enforcement. Assuming the worst happens and incursion takes place, it becomes imperative to detect, contain, and correct the breach. Using a Defense-In-Depth approach reduces an attacker's chance of success while increasing the probability of detection.

The Defense-In-Depth strategy is part of the State's plan to build an infrastructure that protects the confidentiality, integrity, and availability (CIA) of critical information and assets. The goal is to create an architecture that can withstand attacks or disasters of any kind. An infrastructure, employing multiple layers of defense, can be designed to secure the State from losses due to a single incursion.

The State is also aware that it is often more practical to implement multiple, sometimes routine, technologies than it is to depend upon complex, elaborate schemes that potentially include single points of failure. A simple infrastructure is easier to protect, secure, and maintain than a large complex system. While simplicity is not always realistic in a large enterprise like the State of Utah, the State must attempt to develop an architecture that is easy to understand and maintain.

Where a single point of control can become a single point of failure, each layer in a Defense-In-Depth strategy backs up the preceding layer. When incursions occur the outer layers limit the amount of exposure. Multiple layers must be peeled back before valuable assets are fully exposed.

The best strategies provide effective protection of valued assets while allowing commerce to flourish. In addition, the concentric rings of a layered defense, such as the Defense-In-Depth strategy, allow for controlled and monitored access at each layer.

The Depth-in-Defense strategy is composed of the following layers:

- Policy, Procedures, and Awareness
- Physical
- Perimeter
- Network
- Systems
- Applications
- Data

Policies, Procedures, and Awareness

People are the foundation of any good security model. The most secure system is only as secure as the person administrating the system or the users accessing it. At the base of the Defense-In-Depth strategy is the policies, procedures, and awareness that let people know what their roles are and what is expected of them. Methods include:

- Security policies are in place and employees are aware of them.
- Security policies and procedures are reviewed on a regular bases.
- Employees are trained on their responsibilities to ensure the security of systems and data.
- The human factor must be taken into account:
    - Implemented more security processes than technology.
    - People will work around security if it is to complicated
    - People are the weakest link, and the biggest threat is often from within.
    - Employees often can make mistakes and can be careless.
    - Disgruntled, dissatisfied or careless employees can be a threat.
    - Employee awareness, training and education are essential.

Physical (Access and Environment Controls)

This layer wraps around the core components to maintain and control physical access and the environment of the devices. This layer ensures that only appropriate physical access is allowed to the systems. This layer also includes environment controls to ensure that systems do not receive damage from temperature, water, or electrical service failures. Methods include:

- Employees have appropriately badge to enter protected areas.
- Physical locks and controls are in place to prevent access to systems.
- Physical layers or zones in place depending on security requirements.
- Required n-factor authentication to access areas that demand increased security.
- Individual computers and desktops are secured and locked when not in use.
- Environmental controls are in place and monitored to ensure there is no damage to the critical systems.

Perimeter (First Line of Defense Between the Internet and Internal Networks)

This layer is the border between the external world and the internal State network and systems. The perimeter service acts as the hard outer shell that protects all that is inside. This layer must allow traffic and commerce to take place while eliminating as many threats as possible. Methods include:

- Perimeter firewall protection.
- Firewalls between the State's IT assets and the Internet are essential.
- Logging, analysis, and reporting of access.
- Elimination of clear text and other services that can expose internal systems to external threats.
- Encryption of incoming network traffic destined for more secure internal systems, such as:

  - VPN
  - SSL
  - Secure Shell

- Bastion host and proxy services funnel services and limit exposure.
- Proxy cache and other technologies to limit the exposure of internal systems to external services.
- Authentication of employees accessing the network.
- DMZ and filtered networks are in place to only allow external traffic to specified areas and zones.
- Regular vulnerability assessment and penetration testing done to identify weakness and proactively resolve potential problems.

Network (Internal Network Layer)

This layer contains methods to protect the network by monitoring traffic types and segmenting traffic via different security models. These methods include:

- Intrusion detecting and alerting in place to identify proactively respond to problems
- Intrusion prevention systems to allow for automated response to potential security breaches.
- Network traffic shaping and flow to determine patterns and identify potential risks.
- Network segmentation:
  - Separated network via agencies and security levels.
  - VLAN used to separate traffic and limit access between agencies
  - MPLS to tag traffic from individual agencies.

- Access control lists (ACLs) that block traffic and ensures that only those individual IP addresses can access systems and services.
- Non-routable IP addresses are used where possible to keep internal State services from exposure to external networks.
- Internet and Web filtering to protect users from accidentally surfing to inappropriate or hazardous Web sites.
- Network based anti-virus software to eliminate virus and worms before they reach other layers
- Regular vulnerability assessment and testing of network services

Systems (Server and Client Operating System Hardening Practices)

This layer contains methods for standard installation and configuration of operating systems. Those services and programs not specifically needed are not loaded or never turned on. Changes to systems are detected and traced. Change Management processes are used to ensure only appropriate and known changes are made to production systems. Methods used to protect these systems include:

- Establishment of standard configurations across all platforms
- Asset management is implemented to track asset location, use, and disposal.
- Strong authentication and passwords are used
- Change Management and Change Control is rigorously followed and support by all employees.

- Patch management practices are in place to ensure systems are up to the latest possible security patches
- System vulnerability assessments are done constantly to identify possible new vulnerabilities and react quickly.
- Host base intrusion detection and firewall are in place to stop or detect unexpected activity on host systems.
- Anti-virus software is in place and updated on all workstations and servers.

Application (Application Hardening Practices)

This layer contains the applications that run on the host systems and manipulate the data. This layer must ensure that applications do not introduce security vulnerabilities that allow for unauthorized access or unexpected manipulation of data. This layer also must ensure the integrity of data. Methods to protect the application in this layer include:

- Formal change management review and controls.
- An application development life cycle is used and includes a security review.
- Authentication and authorization to application is required
- Logging and auditing of authentication is built into the application.
- E-mail spam and anti-virus filtering are implemented.

Data (Protection of Customer and Private Information)

This layer contains protection and counter measures concerned with protecting the most valuable asset in the infrastructure. This layer contains the data and information that is collected by the State about the citizens and consumers of State services. Methods used to protect data in this layer include:

- Encryption of data when it is transmitted and stored, using multiple technologies, including database encryption.
- Data classification is done to ensure the protection of the most sensitive data.
- Segmentation of data based on required levels of security and confidentially.
    - Don't keep all you eggs in one basket.
- Authentication is required to access data even outside of the application.
- Authorization to access data is based on an individual's role.
- Logging, auditing, and reporting of data access is done
- Access control lists (ACLs) are used to limit access to data based on individual roles.

References

"*Microsoft Security Guidance Training I,*" 2004; Microsoft Corporation.

"*Second Skin*," January 3, 2004; Computer Business Review Online.

"*Survivability: Protecting your Critical Systems,*" 1999; Carnegie Mellon—CERT Coordination Center. www.cert.org

"*The Standard for Good Security Practices for Information Security*," March 2003; Information Security Forum (ISF).